REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-25 are pending in the application. The Examiner additionally stated that claims 1-25 are rejected. By this communication, claims 1, 8, 16, 21, and 25 are amended. Hence, claims 1-25 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Double Patenting Rejections

The Examiner issued provisional rejections of claims 21, 22, and 25 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of copending application No. 10674057 (Docket: CNTR.2224).

With regard to claims 21, 22, and 25, Applicant provides herewith a terminal disclaimer to obviate provisional double patenting rejections over pending "reference" applications that disclaims, except as provided therein, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 10674057 (Docket: CNTR.2224), filed on 9/29/2003, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application.

Accordingly, Applicant respectfully requests that the examiner withdraw the rejections of claims 21, 22, and 25.

The Examiner also issued provisional rejections of claims 1-4, 7-15, 21, 22, and 25 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of copending application No. 10826435 (Docket: CNTR.2075).

With regard to claims 1-4, 7-15, 21, 22, and 25, Applicant provides herewith a terminal disclaimer to obviate provisional double patenting rejections over pending "reference" applications that disclaims, except as provided therein, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 10826435 (Docket: CNTR.2075), filed on 4/16/2004, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application.

Accordingly, Applicant respectfully requests that the examiner withdraw the rejections of claims 1-4, 7-15, 21, 22, and 25.

The Examiner furthermore issued provisional rejections of claims 1-4, 7-15, 21, 22, and 25 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of copending application No. 10727973 (Docket: CNTR.2071).

With regard to claims 1-4, 7-15, 21, 22, and 25, Applicant provides herewith a terminal disclaimer to obviate provisional double patenting rejections over pending "reference" applications that disclaims, except as provided therein, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 10727973 (Docket: CNTR.2071), filed on 12/4/2003, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application.

Accordingly, Applicant respectfully requests that the examiner withdraw the rejections of claims 1-4, 7-15, 21, 22, and 25.

Rejections Under 35 U.S.C. §102(e)

The Examiner rejected claims 1-6, 8-19, and 21-24 under 35 U.S.C. 102(e) as being anticipated by Kessler, US6789147 (hereinafter, "Kessler"). Applicant respectfully traverses the Examiner's rejections.

Referring to claims 1 and 21, the Examiner noted that Kessler discloses a co-processor that includes multiple execution units (Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8). The Examiner noted that this meets the limitation of a cryptographic instruction, received by a computing device as a part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations.

The Examiner also stated that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of wherein said cryptographic instruction prescribes one of a plurality of cryptographic algorithms, algorithm logic, operatively coupled to said cryptographic .instruction, configured to direct said computing device to execute said one of the cryptographic operations according to said one of a plurality of cryptographic algorithms.

The Examiner further observed that using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9, lines 28-43), which meets the limitation of execution logic, operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations.

Applicant appreciates the Examiner's consideration of the noted claims and the points provided above. For ease of reference, claim 1 as amended herein, is provided below.

1. An apparatus for performing cryptographic operations, comprising:

fetch logic, disposed within a microprocessor, configured to receive a cryptographic instruction as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a plurality of cryptographic algorithms;

algorithm logic, disposed within said microprocessor and operatively coupled to said cryptographic instruction, configured to direct microprocessor to execute said one of the cryptographic operations according to said one of a plurality of cryptographic algorithms; and

execution logic, disposed within said microprocessor and operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations.

Applicant has amended claim 1 to clearly recite fetch logic, *disposed within a microprocessor,* configured to receive a cryptographic instruction as part of an instruction flow executing on said microprocessor. These features of the present invention are not taught or suggested by Kessler.

In contrast, Kessler teaches a host processor 202 that communicates with a coprocessor 212 over a system bus 210. Input and output data 208-209 along with requests for cryptographic operations 206 are provided in host memory 204. (Figure 2 and associated discussion). Kessler clearly discloses a coprocessor implementation of a cryptography unit, the limitations and disadvantages of which Applicant has noted and summarized in the instant application in paragraph [0019]. Furthermore, Kessler does not even appreciate the problems associated with such a technique, nor does he provide any motivation for one skilled to provide for a cryptography unit within a microprocessor itself, as has been disclosed in the instant application, and which is recited in claim 1.

One skilled will appreciate that the type of configuration proposed by Kessler is cumbersome in that to provide for encryption and/or decryption of data, a host processor must provide for communication with the coprocessor device via some mechanism over

the system bus that is very slow compared to the speed at which the processor itself could perform the work, if it were configured as is disclosed in the instant application.

In stark contrast, claim 1 recites a cryptographic instruction that is fetched from memory by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recited how the cryptographic instruction prescribes one of a plurality of cryptographic algorithms. Kessler does not teach or suggest an instruction that provides for the foregoing limitations. The claim also recites algorithm logic that is within said microprocessor and operatively coupled to said cryptographic instruction, configured to direct said microprocessor to execute said one of the cryptographic operations according to said one of a plurality of cryptographic algorithms. The claim further recites execution logic that is within the microprocessor as well and that is operatively coupled to said algorithm logic, configured to execute said one of the cryptographic operations. Although Kessler teaches a coprocessor approach to performing these operations, as the Examiner suggests, such operations are not performed in a microprocessor responsive to a cryptographic instruction that is fetched from memory as part of an instruction flow.

Again, Applicant stresses that the approach taught by Kessler is a technique that is employed by hardware *external to a microprocessor*. The apparatus of claim 1, on the other hand, performs cryptographic operations *within a microprocessor, responsive to a cryptographic instruction fetched from memory,* which is advantageous in one aspect in that an instruction is provided for use by a programmer in an application to instruct the microprocessor to perform one of a plurality of cryptographic operations.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

Claim 21 recites substantially the same limitations as have been argued above as being allowable over Kessler. Accordingly, it is requested that the rejection of claim 21 be withdrawn as well

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly,

Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

With respect to claims 22-24, these claims depend from claim 21 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 22-24.

As per claim 16, the Examiner noted that Kessler discloses a co-processor that includes multiple execution units(Figure 2) wherein each of the execution units includes an execution queue to store cryptographic instructions received by the co-processor (Figure 8), which meets the limitation of a cryptographic unit within a device, configured to execute one of the cryptographic operations response to receipt of a cryptographic instruction within an instruction flow that prescribes said one of 'the cryptographic operations. The Examiner additionally observed that the execution units include a plurality of operation blocks that correspond to different cryptographic operations that are used depending upon the type of instruction received in the execution queue (Figure 8 & Col. 9, lines 7-43), which meets the limitation of an algorithm field, configured to prescribed one of a plurality of cryptographic algorithms to be employed when executing said one of the cryptographic operations. The Examiner noted that using the appropriate operation block, the corresponding cryptographic algorithm is used when processing the received instruction (Col. 9, lines 28-43), which meets the limitation of algorithm logic, operatively coupled to said cryptography unit, configured to direct said device to perform said one of the cryptographic operations according to said one of the plurality of cryptographic algorithms.

Applicant respectfully disagrees and directs the Examiner's attention to arguments provided above in traversal of the rejections of claims 1 and 21. More specifically, claim 16, as amended herein, recites, *inter alia,* that the cryptography unit and algorithm logic are both disposed within a microprocessor, and the cryptographic operation, along with corresponding cryptographic algorithm, is specified by a cryptographic instruction that is fetched from memory as part of an instruction flow.

Since these limitations are not taught, contemplated, or suggested by Kessler, it is requested that the rejection of claim 16 be withdrawn.

With respect to claims 17-19, these claims depend from claim 16 and add further limitations that are neither anticipated nor made obvious by Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 16-19.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 7, 20, and 25 under 35 U.S.C. 103(a) as being unpatentable over Kessler, in view of Miller, US6081884. Applicant respectfully traverses the Examiner's rejections.

More specifically, the Examiner noted that Kessler does not specify that the co-processor utilizes the x86 instruction set. However, the Examiner opined that it would have been obvious to one of ordinary skill in the art at the time the invention was made for the co-processor described in Kessler to implement the x86 instruction set because the x86 instruction set has been widely accepted because of it's compatibility with a large amount of software as taught by Miller (Col. 2, lines 9-14).

Applicant respectfully disagrees with the Examiner's points above and notes in the first place that claims 7, 20, and 25 depend from claims 1, 16, and 21, respectively, and add limitations over and above that subject matter which has been previously argued as being allowable over the prior art of record. Applicant also notes, in the second place, that Miller teaches a microprocessor that is optimized to execute *two* instruction sets in a long instruction word (LIW) format. Such a configuration is not according to a single (e.g., x86) instruction format. Miller simply teaches a LIW processor that is backward compatible with x86 applications. In fact, Miller actually teaches away from a cryptographic instruction according to the x86 instruction format because to do so would require using microcode to translate all x86 instructions into RISC or LIW format, noting that this solution typically yields unsatisfactory performance. Applicant disagrees with Miller's assertion regarding performance, but nevertheless maintains that Miller does not provide motivation to include an cryptographic instruction according to the x86 format.

Accordingly, it is requested that the rejections of claims 7, 20, and 25 be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-25 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

10/24/2007

Date: _____